Claims

What is claimed is:

1. A method for securing timestamping of digital data comprising the steps of:
providing a secure encryption key; and,

providing a processor for performing security functions with the secure encryption key, the processor operable in a first mode wherein the secure encryption key is used for encryption operations and for test operations and in a second mode in which the secure encryption key is only used for timestamping operations,

wherein once the processor performs a function with the secure encryption key in the second mode, it is precluded from performing further functions in the first mode with the same secure encryption key.

2. A method for securing timestamping of digital data as defined in claim 1, comprising the steps of:

receiving a request to perform a timestamping operation; and,

placing the processor in the second mode of operation once the request is received.

3. A method for securing timestamping of digital data as defined in claim 2, comprising the step of:

generating a unique code for being embedded within timestamped digital data, wherein the secure encryption key and the processor are within a secure module and wherein the unique code is indeterminable outside the secure module prior to receipt of the request.

4. A method for securing timestamping of digital data as defined in claim 2, comprising the step of generating a unique code for being embedded within timestamped digital data, the unique code being indeterminable before receipt of the request.

5. A method for securing timestamping of digital data as defined in claim 4, wherein the unique code is inserted within each timestamped digital data.

6. A method for securing timestamping of digital data as defined in claim 5, wherein each timestamped digital data comprises a timestamp, and wherein the unique code is encoded within the timestamp.

7. A method for securing timestamping of digital data as defined in claim 3, wherein the unique code is sufficiently large to dissuade brute force attacks.

8. A method for securing timestamping of digital data as defined in claim 7, wherein the unique code is generated based on the secure encryption key.

9. A method for securing timestamping of digital data as defined in claim 7, wherein the unique code is generated based on a random number.

10. A method for securing timestamping of digital data as defined in claim 7, wherein the unique code is generated based on a real time value indicative of a time instance a first request has been received.

11. A method for securely timestamping digital data comprising the steps of:
providing a secure encryption key;

providing a processor for performing security functions with the secure encryption key, the processor operable in a first mode wherein the secure encryption key is used for encryption operations and for test operations and in a second mode in which the secure encryption key is only used for timestamping operations, wherein once the processor performs a function with the secure encryption key in the second mode, it is precluded from performing further functions in the first mode with the secure encryption key;

when the processor is in the first mode of operation, receiving a first request to perform a timestamping operation on first digital data and then placing the processor in the second mode of operation; and,

providing a unique code for being embedded within timestamped digital data, the unique code being indeterminable before receipt of the first request.

12. A method for securely timestamping digital data as defined in claim 11, comprising the steps of:

receiving from a real time clock data indicative of a real time the first request for a timestamping operation has been received;

generating a first timestamp based on the data indicative of real time using the secure encryption key;

embedding the first timestamp within the first digital data and inserting the unique code within the first digital data; and,

encoding the first digital data with inserted data therein to form timestamped digital data.

13. A method for securely timestamping digital data as defined in claim 12 wherein encoding includes the step of encrypting the digital data with the secure key.

14. A method for securely timestamping digital data as defined in claim 13, comprising the steps of:

receiving a second request to perform a timestamping operation on second digital data;

receiving from the real time clock data indicative of a real time the second request for a timestamping operation has been received;

generating a second timestamp based on the data indicative of a real time using the secure encryption key;

embedding the second timestamp within the second digital data and inserting the unique code within the second digital data; and,

encoding the second digital data with inserted data therein to form timestamped digital data.

15. A method for securely timestamping digital data comprising the steps of:

providing a secure encryption key;

providing a processor for performing security functions with the secure encryption key, the processor operable in a first mode wherein the secure encryption key is used for encryption operations and for test operations and in a second mode in which the secure encryption key is

only used for timestamping operations, wherein once the processor performs a function with the secure encryption key in the second mode, it is precluded from performing further functions with the secure encryption key in the first mode;

placing the processor in the second mode of operation; and,

providing a unique code for being embedded within timestamped digital data, the unique code being indeterminable before the processor is placed in the second mode of operation.

16. A method for securely timestamping digital data as defined in claim 15, comprising the steps of:

receiving a request to perform a timestamping operation on digital data;

receiving from a real time clock data indicative of a real time value that the request for a timestamping operation has been received;

generating a timestamp based on the data indicative of a real time using the secure encryption key;

embedding the timestamp within the digital data;

inserting the unique code within the timestamped digital data; and,

encoding the digital data with the unique value and the timestamp embedded therein to form timestamped digital data.

17. A method for securely timestamping digital data as defined in claim 15, comprising the steps of:

receiving a request to perform a timestamping operation on digital data;

receiving from a real time clock data indicative of a real time the request for a timestamping operation has been received;

hashing the digital data; and,

encrypting the hashed digital data with the data indicative of a real time using the secure encryption key.

18. A method for securely timestamping digital data as defined in claim 17. comprising the step of inserting the unique code within the hashed digital data prior to encryption thereof.

19. A method for securely timestamping digital data comprising the steps of:

receiving securely timestamped digital data, wherein the securely timestamped digital data have a unique code embedded therein, and wherein the unique code has been generated by a processor after the processor has been placed in a mode of operation in which a secure encryption key is only used for timestamping operations;

decrypting the timestamp using a key corresponding to the secure encryption key for providing time data in dependence thereupon;

retrieving the unique code from the securely timestamped digital data; and,

comparing the unique code with reference data in order to produce a comparison result, and if the comparison result is indicative of a match indicating authenticity of the time data.

20. A secure system for securely timestamping digital data comprising:

at least a first port for receiving the digital data and for providing timestamped digital data; and

a processor for:

performing security functions with the secure encryption key, the processor operable in a first mode wherein a secure encryption key is used for encryption operations and for test operations and in a second mode in which the secure encryption key is only used for timestamping operations, wherein once the processor performs a function with the secure encryption key in the second mode, it is precluded from performing further functions with the secure encryption key in the first mode.

21. A system for securely timestamping digital data as defined in claim 20, comprising:

a real time clock for providing data indicative of a real time.

22. A system for securely timestamping digital data as defined in claim 21, wherein the processor comprises circuitry for generating a secure encryption key.

23. A system for securely timestamping digital data as defined in claim 22, wherein the processor comprises circuitry for generating a pseudo-random number forming a unique value associated with an encryption key, the unique value for being embedded within each timestamp

formed with the associated key, the unique value being indeterminable outside the system before the processor is placed in the second mode.

24. A system for securely timestamping digital data as defined in claim 22, comprising secure memory for storing the secure encryption key inaccessible outside of the secure system but accessible to the processor for performing security functions therewith, wherein within the memory is stored a unique value associated with an encryption key, the unique value for being embedded within each timestamp formed with the associated key, the unique value being indeterminable outside the system before the processor is placed in the second mode.